



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,581	12/12/2003	Sudarshan Palliyil	JP920030275US1	2542

39903 7590 03/14/2007
ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER

ZEE, EDWARD

ART UNIT	PAPER NUMBER
----------	--------------

2109

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/735,581

Applicant(s)

PALLIYIL ET AL.

Examiner

Edward Zee

Art Unit

2109

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 December 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 12/12/03.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application
- ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing of December 12, 2003. Claims 1-29 are pending and have been considered below.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: "local area network 10". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities: the examiner notes the use of acronyms (ie. DOS, LAN, IT, GSM, WAN, etc.) throughout the specification without first including a description in plain text, as required..

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti (7,143,113).

6. Examiner's Note: The applicant is attempting to invoke 35 U.S.C. 112 6th paragraph in claim 27 by using "means-plus-function" language. However, the examiner notes that the only "means" for performing these cited functions in the specifications appears to be computer program modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other test of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering this claim below.

Claim 1: Radatti discloses a method for identifying data processing systems within a network having a vulnerability, comprising the steps of:

a. computing a set of hash values derived from and representing a set of resources distributed across a plurality of data processing systems within a network(*secure system data file*) [column 3, lines 44-48];

b. storing, at a first data processing system within the network [column 3, lines 44-48], the computed set of hash values together with an identification of the respective one of said

Art Unit: 2109

plurality of data processing systems storing a resource corresponding to each computed hash value [column 4, lines 23-29]. The examiner notes that it is inherent for an identification to be stored with the hash values when different computed hash values(*complete secure system data files and partial secure system data files*) are generated for different users [column 4, lines 23-29].

However, Radatti does not explicitly disclose that in response to an indication that a first resource is associated with a specific vulnerability, comparing at least one hash value representing the first resource with the stored set of hash values to identify matching hash values, and using the identification of matching hash values and the stored identification of respective systems to determine the systems within the plurality of data processing systems storing replicas of the first resource. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to identify all systems storing replicas of the first resource, which has been deemed vulnerable. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claim 2: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 1 above and further discloses that the first resource is a collection of component resources and said at least one hash value comprises a logical combination of hash values representing each of the component resources(*one-to-one correspondence with the files*) [column 4, lines 30-33].

Claims 3 and 4: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 1 above and further discloses that the vulnerability is a vulnerability to a computer virus or computer hacking(*back doors*) [column 6, lines 19-28].

Art Unit: 2109

Claim 5: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 1 above and further discloses classifying the system storing replicas of the first resource as vulnerable [column 7, lines 20-23].

Claim 6: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 1 above and further discloses that a system that has been altered may be restored by replacing the affected file(s) with a known good copy of the file(s) [column 7, lines 59-65], but does not explicitly disclose replacing the replica of the first resource at each of the systems determined to be storing a replica of the first resource. However, it would have been obvious to one of ordinary skill in the art at the time of invention to replace all the replicas of the first resource at each of the systems storing the replica as well. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claim 7: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 1 above and further discloses a system modification tool to restore the system to a secure system state [column 8, lines 61-67], but does not explicitly disclose patching the replica of the first resource at each of the systems determined to be storing a replica of the first resource. However, it would have been obvious to one of ordinary skill in the art at the time of invention to use patching the replica of the first resource at each of the systems storing a replica of the first resource, or any other restoring method. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Art Unit: 2109

Claim 8: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 7 above and further comprises:

- a. patching the replica of the first resource with patch code. The examiner notes it is inherent that a patch code is used when patching a file;
- b. comparing the hashed transmitted content to determine whether the content has maintained pretransmission integrity [column 10, lines 20-24], but does not explicitly disclose comparing a set of hash values representing all pre-requisite programs of the patch code with the stored set of hash values to identify matching hash codes; nor that in response to identification of matching hash codes for all pre-requisite programs, determining that said patching of the replica of the first resource with the patch code should proceed. However, it would have been obvious to one of ordinary skill in the art at the time of invention to verify the integrity of a patch code before proceeding with the patching. One would have been motivated to do so in order to verify that the patch code being used to repair a file has not been compromised during transmission in order to maintain integrity within the system.

Claim 9: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 1 above and further discloses alerting mechanisms [column 7, lines 24-28], but does not explicitly disclose sending a notification of the vulnerability to each system determined to be storing a replica of the first resource. However, it would have been obvious to one of ordinary skill in the art at the time of invention to send a notification to each system that is storing a replica of the first resource, which has been deemed vulnerable. One would have been motivated to do so in order to prevent vulnerabilities from persisting within the network for extensive periods of time.

Art Unit: 2109

Claims 10 and 11: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claims 1 and 9 above and further discloses responding to the determination of respective systems storing replicas of the first resource by selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability(*manually or automatically sending infected file to an antivirus or similar product*) [column 7, lines 30-35], but does not explicitly disclose including the selected instructions within the notification sent to each data processing system and including the step of receiving, from a remote data processing system, at least one hash value representing a first resource associated with a vulnerability together with vulnerability resolution information. However, it would have been obvious to one of ordinary skill in the art at the time of invention to send a hash value representing a first resource associated with a vulnerability and resolution instructions to facilitate the repair. One would have been motivated to do so in order to enable a user to manually restore any compromised files by themselves.

Claim 12: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 11 above but does not explicitly disclose that the vulnerability resolution information comprises at least one program code patch for removing the vulnerability. However, it would have been obvious to one of ordinary skill in the art at the time of invention to use a program code patch for removing the vulnerability or any other method of removing the vulnerability. One would have been motivated to do so in order to reduce consumption of system resources by patching a file to remove the vulnerability instead of replacing the entire file.

Art Unit: 2109

Claims 13 and 14: Radatti discloses a method for identifying data processing systems within a network having a vulnerability as in claim 1 above and further discloses computing the at least one hash value representing the first resource(*secure system data files*) [column 4, lines 23-29], but does not explicitly disclose that it is in response to said indication that the first resource is associated with the vulnerability nor receiving the at least one hash value at the first data processing system together with the indication that the first resource is associated with the vulnerability. However, it would have been obvious to one of ordinary skill in the art at the time of invention to generate the hash value and to receive the hash value at the first data processing system if a vulnerability is discovered. One would have been motivated to do so in order facilitate identifying all the other systems storing replicas of the first resource.

Claim 15: Radatti discloses a data processing apparatus comprising:

- a.. a data processing unit(*controlling computer systems*) [column 3, lines 8-12];
- b. a data storage unit(*storage media*) [column 3, lines 8-12];
- c. a repository manager configured to store a set of hash values and associated system identifiers in a repository within the data storage unit [column 3, lines 44-48], wherein the set of hash values are derived from and represent a set of resources distributed across a plurality of data processing systems and the system identifiers identify particular systems within said plurality of data processing systems at which the resources are stored [column 4, lines 23-29]. The examiner notes that it is inherent for an identification to be stored with the hash values when different computed hash values(*complete secure system data files and partial secure system data files*) are generated for different users [column 4, lines 23-29].

Art Unit: 2109

However, Radatti does not explicitly disclose a vulnerability coordinator configured to respond to an indication that a first resource has a vulnerability, by comparing at least one hash value representing the first resource with the stored set of hash values to identify matching hash values, and configured to use the identification of matching hash values and stored system identifiers to identify systems within the plurality of data processing systems storing replicas of the first resource. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to identify all systems storing replicas of the first resource, which has been deemed vulnerable. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claim 16: Radatti discloses a data processing apparatus as in claim 15 above, but does not explicitly disclose that the vulnerability coordinator is configured to receive at least one hash value representing a first resource from a second data processing apparatus. However, it would have been obvious to one of ordinary skill in the art at the time of invention to generate the hash value and to receive the hash value at the first data processing system if a vulnerability is discovered. One would have been motivated to do so in order facilitate identifying all the other systems storing replicas of the first resource.

Claim 17: Radatti discloses a data processing apparatus as in claim 15 above and further discloses that the vulnerability coordinator is configured to compute at least one hash value representing the first resource(*secure system data files*) [column 4, lines 23-29].

Claim 18: Radatti discloses a distributed data processing system comprising:

- a. a plurality of client data processing systems each comprising a data processing unit and a data storage unit storing resources [column 3, lines 17-25];

Art Unit: 2109

b. a server data processing system comprising a data processing unit [column 3, lines 17-25];

c. a data storage unit(*storage media*) [column 3, lines 8-12];

d. a repository manager configured to store a set of hash values and associated system identifiers in a repository within the data storage unit [column 3, lines 44-48], wherein the set of hash values are derived from and represent a set of resources distributed across a plurality of data processing systems and the system identifiers identify particular systems within said plurality of data processing systems at which the resources are stored [column 4, lines 23-29]. The examiner notes that it is inherent for an identification to be stored with the hash values when different computed hash values(*complete secure system data files and partial secure system data files*) are generated for different users [column 4, lines 23-29].

However, Radatti does not explicitly disclose a vulnerability coordinator configured to respond to an indication that a first resource has a vulnerability, by comparing at least one hash value representing the first resource with the stored set of hash values to identify matching hash values, and configured to use the identification of matching hash values and stored system identifiers to identify systems within the plurality of data processing systems storing replicas of the first resource. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to identify all systems storing replicas of the first resource, which has been deemed vulnerable. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claim 19: Radatti discloses a computer program product, comprising program code recorded on a recording medium, for controlling the performance of operations on a data processing system

Art Unit: 2109

on which the program code executes, the program code comprising a repository manager configured to store a set of hash values and associated system identifiers in a repository within the data storage unit [column 3, lines 44-48], wherein the set of hash values are derived from and represent a set of resources distributed across a plurality of data processing systems and the system identifiers identify particular systems within said plurality of data processing systems at which the resources are stored [column 4, lines 23-29]. The examiner notes that it is inherent for an identification to be stored with the hash values when different computed hash values(*complete secure system data files and partial secure system data files*) are generated for different users [column 4, lines 23-29]. However, Radatti does not explicitly disclose a vulnerability coordinator configured to respond to an indication that a first resource has a vulnerability, by comparing at least one hash value representing the first resource with the stored set of hash values to identify matching hash values, and configured to use the identification of matching hash values and stored system identifiers to identify systems within the plurality of data processing systems storing replicas of the first resource. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to identify all systems storing replicas of the first resource, which has been deemed vulnerable. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claim 20: Radatti discloses a method for determining whether a data processing system has a vulnerability, comprising the steps of:

- a. computing a set of hash values representing a set of resources of the data processing system(*secure system data file*) [column 3, lines 44-48];

b. However, Radatti does not explicitly disclose that for a resource associated with the vulnerability, comparing at least one hash value representing the vulnerability-associated resource with the computed set of hash values, to identify matching hash values and determining, from said identification of matching hash values, whether the data processing system includes the resource associated with the vulnerability. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to identify all systems storing replicas of the resource associated with the vulnerability. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system;

c. in response to determining that the data processing system includes the resource associated with the vulnerability, classifying the data processing system as vulnerable [column 7, lines 20-23].

Claim 21: Radatti discloses a method for determining whether a data processing system has a vulnerability as in claim 20 above and further discloses that in response to determining that the first data processing system includes the resource associated with the vulnerability, retrieving vulnerability-resolution instructions relevant to the vulnerability(*sending infected file to an antivirus or similar product*) [column 7, lines 30-35], but does not explicitly disclose that the data processing system is a first data processing system connectable to a second data processing system, from which the vulnerability-resolution instruction is retrieved, via a network. However, it would have been obvious to one of ordinary skill in the art at the time of invention to include a separate data processing system connected via a network for storing and outputting vulnerability-resolution instructions relevant to the vulnerability. One would have been motivated to do so in

Art Unit: 2109

order to reduce consumption of resources on a users computer by performing various antivirus functions on a separate system.

Claim 22: Radatti discloses a method for determining whether a data processing system has a vulnerability as in claim 21 above, but does not explicitly disclose executing the vulnerability-resolution instructions on the first data processing system. However, it would have been obvious to one of ordinary skill in the art at the time of invention to execute the vulnerability-resolution instructions on the first data processing system. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claim 23: Radatti discloses a method for determining whether a data processing system has a vulnerability as in claim 20 above and further discloses that in response to determining that the first data processing system includes the resource associated with the vulnerability, retrieving patching code relevant to the vulnerability(*sending infected file to an antivirus or similar product*) [column 7, lines 30-35], but does not explicitly disclose that the data processing system is a first data processing system connectable to a second data processing system, from which the patching code is retrieved, via a network. However, it would have been obvious to one of ordinary skill in the art at the time of invention to include a separate data processing system connected via a network for storing and outputting patching code relevant to the vulnerability. One would have been motivated to do so in order to reduce consumption of resources on a users computer by performing various antivirus functions on a separate system.

Claim 24: Radatti discloses a method for determining whether a data processing system has a vulnerability as in claim 23 above, but does not explicitly disclose executing the patching code

Art Unit: 2109

on the first data processing system. However, it would have been obvious to one of ordinary skill in the art at the time of invention to execute the patching code on the first data processing system. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Claim 25: Radatti discloses a method for determining whether a data processing system has a vulnerability as in claim 20 above and further discloses reporting the vulnerability to a vulnerability resolution manager(*report is generated to a system administrator*) [column 7, lines 37-39].

Claim 26: Radatti discloses a computer program product comprising program code recorded on a recording medium for controlling operations within a data processing apparatus, wherein the program code comprises hashing function for generating hash values representing data processing system resources(*secure system data file*) [column 3, lines 44-48], but does not explicitly disclose a vulnerability determination program configured to compare at least one hash value representing a resource associated with a vulnerability with a set of hash values representing resources of the data processing apparatus, thereby to identify matching hash values, and configured to use the identification of matching hash values to determine whether the data processing apparatus includes the resource associated with the vulnerability. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to identify all systems storing replicas of the resource associated with the vulnerability. One would have been motivated to do so in order to increase the security of the system by removing or repairing all points of vulnerability within the system.

Art Unit: 2109

Claim 27: Radatti discloses a computer program product comprising program code recorded on a recording medium for controlling operations within a data processing apparatus as in claim 26 above and further discloses that the vulnerability determination program includes means for generating a vulnerability definition comprising a logical combination of hash values representing resources associated with a vulnerability(*one-to-one correspondence with the files*) [column 4, lines 30-33], but does not explicitly disclose means for comparing the vulnerability definition with the set of hash values representing the resources of the data processing apparatus. However, it would have been obvious to one of ordinary skill in the art at the time of invention to include means for comparing the vulnerability definition with the set of hash values representing the resources of the data processing apparatus. One would have been motivated to do so in order to identify all systems storing replicas of the resource associated with the vulnerability, which would in turn increase the security of the system by removing or repairing all points of vulnerability within the system.

Claim 28: Radatti discloses a computer program product comprising program code recorded on a recording medium for controlling operations within a data processing apparatus as in claim 26 above and further discloses program code for retrieving vulnerability-resolution instructions relevant to the vulnerability(*sending infected file to an antivirus or similar product*) [column 7, lines 30-35], but does not explicitly disclose that it is from a second data processing apparatus. However, it would have been obvious to one of ordinary skill in the art at the time of invention to include a separate data apparatus for storing and outputting vulnerability-resolution instructions relevant to the vulnerability. One would have been motivated to do so in order to reduce

Art Unit: 2109

consumption of resources on a users computer by performing various antivirus functions on a separate system.

Claim 29: Radatti discloses a computer program product comprising program code recorded on a recording medium for controlling operations within a data processing apparatus as in claim 26 above and further discloses program code for retrieving patching code relevant to the vulnerability(*sending infected file to an antivirus or similar product*) [column 7, lines 30-35], but does not explicitly disclose that it is from the second data processing system. However, it would have been obvious to one of ordinary skill in the art at the time of invention to include a separate data apparatus for storing and outputting patching code relevant to the vulnerability. One would have been motivated to do so in order to reduce consumption of resources on a users computer by performing various antivirus functions on a separate system.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Fisher et al. (6,092,189), Waldin et al. (6,094,731), Slivka et al. (6,049,671) and Cambridge (7,080,000).

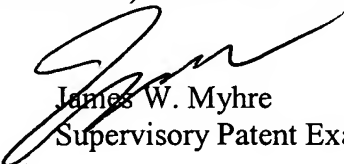
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 6:30AM-5:00PM EST.

Art Unit: 2109

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James W. Myhre can be reached on (571) 270-1065. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
EZ
March 6, 2007


James W. Myhre
Supervisory Patent Examiner
